## REMARKS

The following arguments are presented for the Examiner's consideration. The claims have not been further amended.

The invention as defined by the claims is a dual function random number generator and stream cipher generator. The device has a crypto-engine that can operate as either a random number generator or a stream cipher generator. A controller for controlling whether the crypto-engine operates either as the random number generator or the stream cipher generator has three multiplexers. The first two multiplexers control input signals to the crypto-engine and the third the output of the crypto-engine. The first multiplexer is arranged to receive a random number generator seed signal and a stream cipher generator key signal. The second multiplexer is arranged to receive a dynamic synchronization signal and a constant synchronization signal. The third multiplexer is arranged to receive an output signal from the crypto-engine and provide a random number output or a stream cipher output. When the crypto-engine is to act as a random number generator the first and second multiplexers are controlled to provide the random number generator seed signal and the dynamic synchronization signal inputs to the crypto-engine. The output from the third multiplexer is controlled to be the random number output. When the crypto-engine is to act as a stream cipher generator the first and second multiplexers are controlled to provide the stream cipher generator key signal and the constant synchronization signal inputs to the crypto-engine. The output from the third multiplexer is controlled to be the stream cipher output.

In the rejection Djakovic is relied on as teaching a crypto-engine operable as either a random number generator or a stream cipher generator and Ozluturk as teaching a controller (e.g., switch) for controlling the crypto-engine to operate either as the random number generator

or the stream cipher generator. Further, Vobach and Degele are relied on as teaching a random number generator seed signal and synchronization signals. It is respectfully submitted that no combination of the citations meets the strict requirement of disclosing every element of the claimed invention.

The reason Djakovic is silent about a controller for controlling the crypto-engine to operate either as the random number generator or the stream cipher generator is because Djakovic does not teach a crypto-engine operable as either a random number generator or a stream cipher generator.

Djakovic relates to improving the security of block ciphers using cipher concatenation in combination with a random number generator. The title to Djakovic is Cipher Mixer with **Random Number Generator** [emphasis added]. The abstract of Djakovic begins: [a]n encryption device has a **random number generator** [emphasis added].

Djakovic teaches, as is well known, that the strength of a cipher is improved with greater key length, but that concatenation or combined of block ciphers may not effectively increase the key length because double encryption with two separate 128-bit keys, for example, does not provide effective 256-bit key encryption. At column 1 line 47 to 55 Djakovic describes a prior art method of effectively combining cipher blocks by generating a random number R the same length as the text M to be encrypted. The random number is encrypted by the first cipher block. The output of the first cipher black is combined with the text M in an exclusive-or and the exclusive-or output encrypted by the second cipher block.

Djakovic further explains at column 1 line 63 to 65 that combining multiple ciphers can have a problem in that the combination is potentially weakened if one of the component ciphers is compromised and the combination may be only as strong as only one of the elements (ciphers)

in the combination. The object of Djakovic is to produce block ciphers from existing, already accepted block ciphers as components because there is already a built up trust in the components. A cipher mechanism (10) (e.g. a crypto-engine) that achieves this object is shown in Figures 1 and 2 and described at column 3 line 20 through column 4 line 20 of Djakovic. The cipher mechanism (10) has a random number generator (14) coupled to a cipher mixer (12). The cipher mixer (12) comprises three block cipher mechanisms (18, 20, 22). The random number generator output is used to combine the block cipher mechanisms 18 and 20 using an exclusive-or. The output of the random number generator is encrypted by cipher block (22) and combining with the output of the second cipher block (20).

Further, at column 6 lines 27 to 29 Djakovic teaches that the cipher mechanisms can be on the same chip, but that it is preferably to use of a separate, commercially available, random number generator. Thus, the ciphers and random number generator are separate mechanisms and the crypto-engine is not operable as a random number generator, which is an entirely separate element.

Djakovic clearly teaches that the device operates only as a crypto-engine and the random number generator is used as part of the encryption process. There is no teaching or suggestion in Djakovic that the device operates as either a random number generator or a stream cipher generator. The difference is significant. Therefore, even if Djakovic were modified with Ozluturk, the invention defined by claims could not be produced.

Djakovic does not have a controller, nor multiplexers (switches) controlled by the controller to supply signals selectively to and receive signals from the crypto-engine.

Ozluturk has switches and impliedly a controller for the switches. However, Ozluturk relates to encryption in a Code Division Multiple Access (CDMA) system for transmission of

both voice and data. The switches (14, 190) in Ozluturk are provided for the purpose of selecting between the voice and data inputs and outputs. The two switches are not connected to nor related to the operation of the cipher 17 or its key 18 and so do not supply signals selectively to and receive signals from the crypto-engine as required by the instant claims.

Next, while Vobach and Degele teach a seed signal for a random number generator, but they do not teach dynamic and constant synchronization signals. Teaching that outputs must be synchronized (column 1 lines 43 to 52 of Vobach) does not teach providing a dynamic synchronization signal and constant synchronization signal.

Even if Ozluturk is combined with Vobach and Degele the combination does not teach every features of the claimed combination "a controller controlling the crypto-engine... including three multiplexers controlled by the controller to supply signals selectively to and receive signals from the crypto-engine, in which a first multiplexer is arranged to receive a random number generator seed signal and a stream cipher generator key signal, a second multiplexer is arranged to receive a dynamic synchronization signal and a constant synchronization signal, and a third multiplexer is arranged to receive an output signal from the crypto-engine and provide a random number output or a stream cipher output." Therefore, even if Djakovic were combined with the teaching of Ozluturk and modified by Vobach and Degele the invention defined by claims would not result.

It is apparent from the foregoing description of the publications applied in rejecting the examined claims, that no combination of those publications can disclose or suggest the invention as defined by the claims. Accordingly, upon reconsideration, all of those claims should be allowed.

Respectfully submitted,
JACKSON WALKER L.L.P.

Thomas E. Sisson
Reg. No. 29,348
112 E. Pecan Street, Suite 2100
San Antonio, Texas 78205
Phone: (210) 978-7700
Fax: (210) 978-7790
Attorneys for Applicant

**CERTIFICATE OF MAILING**

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited on the date shown below with the United States Postal Service, with sufficient postage (37 CFR 1.8(a)), in an envelope addressed to Mail Stop: RESPONSE/NO FEE, Commissioner of Patents, P. O. Box 1450, Alexandria, VA 22313-1450.

Via First Class Mail

Date: August 8, 2005

Shirley McIntyre